REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 22-10-2009	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Computer Network Operations Command and Control:
A New Perspective

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Shane M. Connary, Lt Col, USAF

Paper Advisor: Richard M. Crowell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT. The 2009 Quadrennial Roles and Missions Review Report states "Experience from recent operations and global cyberspace incidents underscore the critical role cyberspace capabilities play in preventing conflict when possible, and supporting full-spectrum military operations when necessary…Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time." The standup of United States Cyber Command in September 2009 was a milestone in cyberspace command and control (C2). However, the DOD continues to struggle in developing the proper doctrine, organizations, and processes to execute the cyberspace mission across the range of military operations. Current doctrine has not kept pace with the technological and intellectual advancements of cyberspace. Using a cyber scenario as a backdrop, this paper examines some of the complex challenges operational commanders face concerning cyberspace C2. It discusses current doctrine disconnects, Computer Network Operations fundamentals, the information environment and cyberspace's role in it, as well as the levels of warfare. Finally, the paper contrasts two possible models for cyberspace C2 at the operational level of command, and provides recommendations to meet the cyberspace challenges.

15. SUBJECT TERMS

Computer Network Operations (CNO), Cyberspace, Command and Control (C2), USCYBERCOM

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		28	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

Computer Network Operations Command and Control: A New Perspective

by

Shane M. Connary

Lt Col USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ____________________

22 October 2009

Contents

Introduction 1

Doctrine Disconnects 4

CNO Fundamentals 6

Information Environment and Cyberspace's Role 8

Levels of War 10

Establishment of USCYBERCOM 11

Operational C2 12

Recommendations/Conclusions 16

Notes 18

Appendix A 22

Bibliography 24

Abstract

The 2009 Quadrennial Roles and Missions Review Report states ―experience from recent operations and global cyberspace incidents underscore the critical role cyberspace capabilities play in preventing conflict when possible, and supporting full-spectrum military operations when necessary…Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time."[1] The standup of United States Cyber Command in September 2009 was a milestone in cyberspace command and control (C2). However, the DOD continues to struggle in developing the proper doctrine, organizations, and processes to execute the cyberspace mission across the range of military operations. Current doctrine has not kept pace with the technological and intellectual advancements of cyberspace. Using a cyber scenario as a backdrop, this paper examines some of the complex challenges operational commanders face concerning cyberspace C2. It discusses current doctrine disconnects, Computer Network Operations fundamentals, the information environment and cyberspace's role in it, as well as the levels of warfare. Finally, the paper contrasts two possible models for cyberspace C2 at the operational level of command, and provides recommendations to meet cyberspace challenges.

INTRODUCTION

Fact or Fiction: North Publica executes Operation EAGLE HUMILIATION.[2]

Phase I – Exploitation: North Publica (NP) is the most recent rogue nation added to the United States' Axis of Evil list. NP's current anti-American operation executes a high-visibility attack against the United States while setting up al-Qaeda (AQ) for retribution. For over eight months, NP carried out cyber exploitation against a utility company in Guam while a small Special Forces (SF) unit exercised associated urban terrorist tactics. The cyber exploitation was targeted against a utility company (Quality Electric-QE) providing power to the island.

QE believed they had a secure network; the power plant's computer system was ―air gapped" from the internet. However, QE connected their internal administrative network to the plant's supervisory control and data acquisition (SCADA) system for direct real-time access to improve business efficiency and effectiveness.[3] Through human intelligence, NP determined the QE operation's manager was a Pittsburgh Steelers Fan and visited various football internet sites. Through a series of social engineering techniques, NP operatives befriended the manager on-line. The NP team exchanged stories and later video clips. When the QE executive viewed the video, it downloaded to his hard drive, and when his desktop search program indexed the file, a Trojan horse executed.[4] The exploitation program searched his hard drive for information on access to the SCADA system and sent vital data back to NP through a safe ―dead-drop" email location. Within a very short time, NP established an administrator-level account on the QE network. Over several months, NP mapped the network to establish a topography to understand the network nodes and vulnerabilities. NP also succeeded in gaining needed access to the SCADA system.

Phase II – Cyber Execution: On 26 November, NP executed its well-planned operation. The first step was to shutdown power to the tourist area near Tumon Beach. To help conceal its identity, NP cyber warriors used anonymizer techniques. In this case, they used onion routing to disguise the source of the remote cyberattack.[5] NP routed the command to disrupt the QE SCADA through a number of countries to include Australia, France, Russia, Indonesia, and finally the United States. The final command would look like it came from a location in California and would leave pointers back through routers to a known AQ operating location in Southeast Asia. Additionally, the NP ―hacked" an AQ website and posted a statement claiming AQ was responsible for the Guam attacks.

The direct effect of the cyberattack was to activate a pre-positioned program in the company's computer to disrupt normal operations. The indirect effect was to interrupt the electric power for the northwest portion of Guam. However, an unintended effect was to cycle power switchgear, which overheated several generator system processors. The generators then shutdown and caused a blackout throughout the island including several hospitals. NP leaders understood cyber operations would have both intended and unintended consequences.[6] Although the NP leaders did not plan for these unintended outages, it played into their larger information operation to terrorize and humiliate the United States.

Phase III – Urban Operations: The NP SF kicked off their urban terrorist operations as soon as the lights went black in the Tumon Bay tourist district. The plan called for traditional terrorist and kinetic operations, but the team employed cutting-edge technology and cyberspace operations to execute the mission.[7] The SF initially used the internet and Google Earth maps to survey the area and determine target sets.[8] The 10 NP terrorists carried AK-47s and knapsacks loaded with explosives and plastic bags filled with food, amphetamines, and grenades.[9] They split-up and went after several high-value targets to include a prominent five-star hotel. Each of the SF units communicated with their NP handlers in real-time by satellite phones. At the hotel, they used their phones and Voice over Internet Protocol (VoIP) to discuss operations and relay victim information with the NP command center.[10] In real-time, center personnel would then use the internet to verify victim identification and pass further instructions.[11] As siege at the hotel continued, the handlers even provided updates to the terrorists based on information they received over international news broadcasts such as CNN.[12] After 60 hours and 172 dead, the local police captured one and killed nine of the terrorists.[13]

The above North Publica scenario is both fact and fiction. North Publica is, of course, fictional but it could be any number of nation states or terrorist/criminal groups. Additionally, Phase I and II of Operation EAGLE HUMILIATION were fictional. However, a relatively sophisticated group of cyber warriors could execute the underlying technologies and possibly a similar mission. Phase III is fact; this operation was carried out over several days by the Lashkar-e-Taibi (LeT) terrorist group in November 2008 in Mumbai, India.[14]

The scenario highlights just a few of the complex issues facing Department of Defense (DOD) senior leaders as they develop cyberspace doctrine, organizations, and processes. The 2006 National Military Strategy for Cyberspace Operations (NMS-CO) states, ―The United States operates in a global environment characterized by interdependence, uncertainty, complexity, and continual change."[15] This is especially true for cyberspace where the military went from stand-alone computers processing administrative actions to net-centric weapon system platforms accomplishing crucial missions and the standup of a Sub-Unified Command to oversee a new domain in less than two decades. The DOD is now ―all in" across the Range of Military Operations (ROMO) when it comes to Computer Network Operations (CNO).[16]

The DOD made considerable progress in its initial efforts to address operations in the domain of cyberspace. However, the DOD continues to struggle in developing the proper doctrine, organizations, and processes to execute the complex cyberspace mission. Current doctrine has not kept pace with the technological and intellectual advancements of cyberspace. Furthermore, organizations continue to change and adapt to the cyberspace environment. The standup of United States Cyber Command (USCYBERCOM) in September 2009 was a significant milestone in cyberspace command and control (C2).

Due to the unique domain of cyberspace, the sub-unified commander should execute operational C2 of cyber forces under a Joint Functional Component Command for Cyber (JFCC-Cyber) model versus a Joint Force Commander (JFC) executing through a Joint Force Cyberspace Component Commander (JFCCC). Using the NP scenario as a backdrop, this paper examines some of the challenges operational commanders face that drive cyberspace C2. It will discuss current doctrine disconnects, CNO fundamentals, the information environment and cyberspace's role in it, as well as the levels of warfare. The paper finally contrasts two possible models (noted above) for cyberspace C2 at the operational level of command, and provides recommendations to meet cyberspace challenges.

DOCTRINE DISCONNECTS

Current DOD cyberspace doctrine is in its infancy. Much of the doctrine is based on CNO's place within the larger framework of Information Operations (IO).[17] However, cyber doctrine is adapting and growing. Influential documents such as the 2009 DOD Quadrennial Roles and Missions Review Report (QRM) and 2006 NMS-CO provide insight beyond the

Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-13, *Information Operations*. Furthermore, computer systems are now pervasive throughout DOD mission areas.[18] As network technology advances and CNO expands, new vulnerabilities and opportunities arise.[19]

General James Cartwright, as the Acting CJCS, published a new definition of cyberspace operations on 18 August 2009. He states, cyberspace operations are –the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[20] The CJCS description builds on the definition of cyberspace in the 2009 QRM. The QRM describes –cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[21] The report's definition establishes a clear and general understanding of cyberspace's composition. The two combined definitions provide foundational insight into the current definition of CNO and set the stage to discuss doctrine disconnects.

Current Joint Doctrine characterizes CNO as one of the five core capabilities of IO.[22] CNO is lumped together with the disparate areas of Psychological Operations, Military Deception, Operations Security, and Electronic Warfare due to commonalities in the information environment.[23] The doctrine suggests the ultimate objective of *each* core IO area is to influence a decision maker to act (or not act) in a specific manner. However, General Alexander, the new USCYBERCOM commander, noted, –the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace. Granted, by denying enemies' freedom of action in cyberspace, we will also influence them; however, influence is not the intended primary effect—denying freedom of action is the primary effect."[24] This doctrinally separates cyber operations from the other IO capabilities. Furthermore, cyberspace's growth has positioned it in a place of preeminence as compared to its brother IO core capabilities.

CNO FUNDAMENTALS

Joint doctrine breaks CNO into three distinct military operational areas: Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).[25] Joint Pub 3-13 defines CNA as ―actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[26] CNA can also be described in a broader concept of cyberattack.[27] Cyberattack alters, disrupts, deceives, degrades, or destroys an adversary's computer system or network or information and/or programs resident in or transiting the systems or networks.[28] More specifically, the NMS-CO describes cyberattack operations as, ―DOD will execute the full ROMO in and through cyberspace to defeat, dissuade, and deter threats against US interests."[29]

One should view CNE as an enabling capability of CNA; a cyber warrior will likely be in a position to exploit first and then potentially attack. Current doctrine describes CNE as ―enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[30] Again, CNE may be addressed in a broader context as cyberexploitation.[31] Cyberexploitation supports the ―goals and missions of the party conducting the exploitation, usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks. Cyberexploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view—indeed, the best cyberexploitation is one that such a user never notices."[32] Additionally, the timeframe for cyberexploitation is substantial, usually measured in weeks or months. Finally, the NMS-CO puts it in military specific terms by stating, ―DOD will use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive operations."[33]

There is a clear link between attack and exploitation, but the relationship can be complex. CNE is usually the first step needed for CNA. CNA and CNE are not, however, mutually exclusive options—destroy the computer/network or exploit it. In fact, destroying the computer/network ―may also reveal to the adversary some vulnerability or access path previously unknown to him, and thus compromise friendly sources and methods."[34] The transition between the two can be smooth. For example, a CNE tool could have imbedded CNA capabilities for possible later execution.[35] On 16 September 2009, RDML William Leigher discussed an operational CNE/CNA process model at the Naval War College. Figure 1 in appendix A depicts an author enhanced CNE/CNA process based on the lecture.[36]

Although CND is a critical element of cyberspace operations, it is beyond the focus of this research. In this context, one should understand CND's role as the third leg of the CNO stool. Joint Pub 3-13 defines CND as ―actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks."[37] CND can be either active or passive defense. In some cases, active defense could mean using CNA to defensively eliminate threats.[38] For example, if the DOD confirmed it was the target of a cyberattack, the DOD could (hypothetically) execute a botnet counterattack employing distributed denial of service (DDOS) at the threat.[39]

The NP cyber warriors understood the fundamentals of CNE and CNA. They expertly employed social engineering and then cyberexploitation to map QE's network topology. When the time came, they executed a relatively sophisticated cyberattack that covered their electronic tracks. They also clearly understood cyberattack could be especially effective when used in conjunction with kinetic attacks or other operations. Finally, the terrorists understood they could meet their strategic IO goals with a series of tactical actions.[40] They focused on all three aspects of the information environment.

INFORMATION ENVIRONMENT AND CYBERSPACE'S ROLE

It is important to understand the information environment and cyberspace's role within it when examining possible C2 constructs. Even though cyberspace is disconnected from the other IO core capabilities, it still shares the same attributes of the information environment. Joint Pub 3-13 describes the information environment as:

> The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information…where humans and automated systems observe, orient, decide, and act upon information…it resides within each of the four domains. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.[41]

The physical dimension of the information environment contains cyber hardware and infrastructure. It includes items such as C2 systems and networks, computers and communications systems, and the related infrastructure.[42] The information dimension contains ―information that is processed, stored, disseminated, displayed, and protected; all of which are important functions that take place within cyberspace."[43] The cognitive dimension encompasses the mind of the target audience and is where people think, perceive, visualize, and decide.[44] Again, influencing a target audience within the cognitive dimension could be a critical indirect effect of a cyberattack. The links to IO are strong, but cyberspace is a domain unlike the other IO core capabilities.

The debate concerning cyberspace being a domain is essentially over.[45] General Chilton, Commander of United States Strategic Command (USSTRATCOM) unequivocally stated, ―cyberspace has emerged as a global war-fighting domain—a domain that is as critical to ensuring our national security as its companion domains of land, space, sea, and air."[46] General Alexander advocated cyberspace cross-domain integration when he stated, ―When we conduct any military operation, we must integrate and synchronize all available instruments of warfare in all domains."[47]

However, the intellectual transition of cyberspace from a function to a domain remains a challenge for some planners and leaders. These misguided warriors want to continue to treat cyberspace as a disparate set of missions or functional areas to be spread across the services and DOD agencies.[48] Former Secretary of the Air Force, Michael Wynne, summed up the debate best when he stated, ―The cyber realm embodies far more than just network warfare. Cyberspace is a domain, like land, where each of the principles of war applies. To grasp this concept requires a major institutional and cultural shift in war planning and operations."[49]

The NP cyber warriors integrated and synchronized their cyber and SF operations to bring about strategic level effects. The bold Mumbai attacks, broadcast on international television, had global ramifications. Simply executing the tactical blackout operations would have had similar strategic impacts. However, the blackout attacks alone may have had diminished cognitive impacts on the target audience (American population). The terrorists understood how CNO transcends the levels of warfare from tactical to strategic.

LEVELS OF WAR

Comprehending the levels of war and how cyberspace transcends them is essential to building an effective C2 construct. Dr. Milan Vego links the three levels of war--tactical, operational, and strategic--to the scale and complexity of the objective to be accomplished.[50] He explains, ―In a physical sense, there are, of course, no ―levels," but only different sizes of physical space and mediums (land, sea, air/space) in which friendly and enemy forces operate."[51] Cyberspace, however, is not restricted by the same physical boundaries as the domains of land, sea, air, or space.[52] These differences require a unique mindset. The types of weapons and access to them also support that the cyberspace domain must be treated differently.

The barriers to entry for CNO are minimal. Many of the ―technologies are inexpensive and easily available to non-state actors, including individuals, and these technologies include some that are as capable of doing great harm as those available to governments."[53] In the domain of cyberspace, a weapon of mass destruction may be a single hacker's computer controlling a million-plus computer botnet. Furthermore, the technical expertise to execute cyberattacks effectively is prevalent.[54] With a small investment, hackers have caused millions of dollars of damage and operational/strategic effects.[55]

Cyberattacks are much like the United States Marine Corps' concept of the ―strategic corporal."[56] A Marine in the field at the tactical level can have strategic effects, especially in a counterinsurgency operation. Dr. Vego addresses this concept when he notes, ―All of the levels of war are interrelated; actions and activities at each level affect the other levels…decisions made at the tactical level have considerable and sometimes significant impact on events at the operational and even strategic levels of war. Sometimes tactical events cause a significant ripple effect at the operational and strategic levels of war."[57]

Furthermore, the United States reliance on cyberspace provides an enemy cyber warrior opportunity to attack at the operational or strategic level.[58] As in the NP scenario, a tactical attack can have strategic effects when targeted against high-value infrastructure targets. This reliance on cyberspace drove senior government leaders to adopt a new organization to oversee the domain.

ESTABLISHMENT OF USCYBERCOM

Today, almost every facet of American society relies on cyberspace.[59] For the military, cyberspace became critical to execute C2, intelligence, communications, planning, and mission operations.[60] Additionally, our dependence on cyberspace and net-centric activities continue to grow at a rapid rate.[61] Out of this setting came the birth of USCYBERCOM.

On 23 June 2009, Secretary of Defense Gates signed a memo establishing a Subordinate Unified USCYBERCOM under USSTRATCOM to execute military cyberspace operations.[62] He addresses the critical need by stating, ―our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the DOD requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations."[63]

The new organization pulls together offensive and defensive cyber expertise across the DOD. The direction disestablishes the Joint Task Force-Global Network Operations and

Joint Functional Component Command-Network Warfare and reestablishes the functions at USCYBERCOM no later than October 2010.[64] It also directs the CJCS to develop an implementation plan to delineate ―mission, roles and responsibilities, command and control, reporting and support relationships with combatant commands, Services, and U.S. Government departments and agencies."[65] Developing and executing an effective C2 construct is critical due to the unique characteristics of the cyberspace domain.

OPERATIONAL C2

The NP scenario provided basic insight into the complex variables associated with CNO C2. From mission planning, execution of exploitation and attack, to determining attribution, an operational commander must fully comprehend the cyberspace domain. The commander also requires integration of organizations, capabilities, functions, technologies, and missions to achieve the desired effects in and through cyberspace.[66]

Against the NMS-CO backdrop and the standup of USCYBERCOM, the paper will now examine two new models for cyberspace C2. The first model is placing a Joint Force Cyberspace Component Commander (JFCCC), much like a Joint Force Air Component Commander (JFACC), under a Joint Force Commander (JFC).[67] Air Force doctrine notes that a JFACC ―focused on the broader aspects of an operation, can best mediate the competing demands for tactical support against the strategic and operational requirements of the conflict."[68] The JFCCC would act in a similar manner for cyberspace operations and would be located at the JFC headquarters.

The second model is a Joint Functional Component Command for Cyber (JFCC-Cyber) similar to the current JFCC-SPACE. The ―JFCC-SPACE continuously coordinates, plans, integrates, commands and controls space operations to provide tailored, responsive, local and global effects, and on order, denies the enemy the same, in support of national, USSTRATCOM and combatant commander objectives.”[69] Furthermore, the Commander, JFCC-SPACE using the capabilities inherent in the Joint Space Operations Center (JSpOC) –serves as the single point of contact for military space operational matters to plan, task, direct, assess, and execute space operations.”[70] In this case, the JFCC-Cyber and an associated Joint Cyber Operations Center (JCyOC) would be located at USCYBERCOM.

The two models each have strengths and weaknesses for executing CNO. Although an operational commander has many cyberspace C2 requirements, this paper will compare and contrast the models against only five key requirements—specialized knowledge, coordination, time, attribution determination, and operational vision. Each of the models will be rated as high, medium, or low on how well it meets the requirement.

As described in the NP scenario, CNO is very complex to plan and execute. Cyberattacks –can involve a much larger range of options than most military operations, and because they are fundamentally about an attack’s secondary and tertiary effects, there are many more possible outcome paths whose analysis often requires highly specialized knowledge.”[71] Additionally, the CNO planning effort may require –enormous amounts of intellectual coordination among different individuals.”[72] Due to a JFC’s limited force structure, a JFCCC would likely have a small staff with limited dedicated cyber-knowledge resources. Executing a cyberattack without fully comprehending the many possible effects could have devastating strategic impacts. The JFCCC would need reach-back capability to meet his specialized knowledge requirement, which could impact operational timing (see below). Using the JCyOC and resident National Security Agency assets, the JFCC-Cyber would have a robust base of cyber knowledge to tap. Capability rating: JFCCC, low; JFCC-Cyber, high.

The NMS-CO noted that CNO requires a great level of coordination and synchronization.[73] Partnerships and strong relationships are necessary not only between DOD organizations, but also within the United States Government, the private sector, and allied nations.[74] Specifically within the government, partnerships are needed with the ―Intelligence Community, Department of Justice, Department of Homeland Security, and other Federal departments."[75] At the JFCCC, manpower constraints may negate having a large organization with multiple liaisons from across this wide spectrum of organizations. It may be possible to pull together the full team at one JFC staff, but to replicate this across theaters or Geographic Combatant Commands (GCC) would be near impossible. The JFCCC would need to use reach-back for coordination. The JFCC-Cyber's organization (and JCyOC) is built upon having all the required organizations participate as part of its daily operational routine. Its cross-cutting team should be staffed and equipped to address issues from the multiple entities. Capability rating: JFCCC, medium; JFCC-Cyber, high.

Time is a significant issue when executing all three legs of the CNO stool. In fact, ―the time scales on which cyberattacks operate can range from tenth of a second to years."[76] The NP scenario highlights that a cyberexploitation operation could take months to establish and could then be active for weeks, months, or years. Additionally, reaction time for CND is a concern. If the attacking computer cuts the transmission path or goes dark before it is traced, the opportunity for counter-attack may be difficult or impossible.[77] The organization must be flexible and adapt to the factor of time. The time requirement also links back to the organization having the wherewithal and expertise to react to each CNO area. In either model, a JFC must provide cyber mission requirements with long-lead time as soon as possible to the planning process. The JFCC will not have in-house capabilities to execute either the CNE or CNA mission.[78] The JFCC-Cyber may have limited in-house CNE/CNA capabilities in the JCyOC, but would have operational and tactical control of component units accomplishing the missions. This relationship should provide greater insight and reaction speed. Capability rating: JFCCC, low; JFCC-Cyber, medium.

Attribution is the process of trying to identify the party responsible for a cyberattack.[79] Proper attribution must be accomplished prior to any consideration of retribution. Again, the relationship between cyberexploitation and cyberattack is very complex—one could easily perceive exploitation as attack. The NP case provides several ―hooks” for the DOD to grab during the attribution process.[80] A few of the attribution questions (as discussed by Owens, et al) an operational commander must consider are in appendix A, Table 1.[81] Both C2 constructs will be challenged to quickly and effectively meet the attribution determination requirement. The specialized resources of the JCyOC should provide an advantage over the JFCCC's operations center in-house assets. The ―all-source” capabilities in the JCyOC are built upon the partnerships noted above.[82] Capability rating: JFCCC, low; JFCC-Cyber, medium.

Finally, any operational cyber C2 construct should contribute to the commander's operational vision. Understanding what is happening within the domain and possible effects on operations is critical. Having a solid operational awareness also provides insight and clarity to the requirements of coordination, time, and attribution. Because there are no geographic lines or boundaries to cyberspace, a JFCCC focusing on a specific theater or area of operations will likely have a more restricted site picture. Reach-back capability will greatly support the effort, but subtle connections between cyber events could be missed. Issues with highly-classified and compartmented CNO operations may also limit some knowledge. A primary objective of the JCyOC is to provide JFCC-Cyber with operational details of missions across the domain (and globe). Capability rating: JFCCC, medium; JFCC-Cyber, high.

Based on a comparison of results (appendix A, Table 2), the JFCC-Cyber model outperforms the JFCCC model. However, each cyber C2 construct still has weaknesses that will challenge an operational commander. By centralizing the command and control of cyberspace, the JFCC-Cyber model better harnesses the capabilities of this unique domain.

RECOMMENDATIONS/CONCLUSIONS

This essay began with a fictional adaptation of a real world terrorist incident. The LeT leveraged cyberspace throughout their devastating 2008 Mumbai rampage. The scenario highlighted complex issues facing DOD leaders as they develop cyberspace doctrine, organizations, and processes across the ROMO. The 2009 QRM stated ―Experience from recent operations and global cyberspace incidents underscore the critical role cyberspace capabilities play in preventing conflict when possible, and supporting full-spectrum military operations when necessary."[83] To meet the challenge, DOD and USCYBERCOM should adopt the below recommendations.

The standup of USCYBERCOM in September 2009 was a significant DOD cyberspace milestone. The CJCS must now develop a plan to delineate ―mission, roles and responsibilities, command and control, reporting and support relationships…" for a full operating capability not later than October 2010.[84] Although the operational C2 construct of a JFCC-Cyber is more effective than a JFCCC, the JFCC-Cyber model is unlikely to be integrated into the on-going USCYBERCOM C2 plan. The sub-unified commander will not want to add additional layers of organizational bureaucracy. However, USCYBERCOM can learn valuable lessons from the highly successful JFCC-SPACE construct. The standup of the JSpOC and its partnerships provide an opportunity to gain vital insight. USCYBERCOM should take advantage of JFCC-SPACE lessons learned from space's last decade of growth.[85]

The second recommendation is to create dedicated cyberspace doctrine versus using the current embedded IO doctrine. General Alexander noted, ―while we have ample national level strategies, we have yet to translate these strategies into operational art through development of joint doctrine for cyberspace."[86] Joint level doctrine will provide foundational guidance for all Services and DOD agencies to build upon.

Finally, two cyberspace topics require additional research to enhance cyber processes and organizations. First, a paper should focus on why a C2 construct must fully take into account the JFC's requirements. The JFC is the ultimate customer and should have the final input on any CNO in their area of responsibility. Furthermore, a second paper should address USCYBERCOM wargaming and why it is vital for organizational TTPs. The wargames should include joint, interagency, and allied partners in full-play events. As seen in the NP scenario, the intellectual heavy-lifting and coordination between organizations must be addressed before the time-critical event occurs.

The DOD must take these actions now to meet the ever-expanding domain of cyberspace. Our adversaries, whether nation states, terrorists, or international criminal groups, have adopted cyber operations as part of their asymmetric tactics against the United States. ―Our national security is inextricably linked to the cyberspace domain" and it is up to USCYBERCOM to lead the charge to gain and maintain cyberspace superiority.[87]

END NOTES

1. U.S. Department of Defense, *Quadrennial Roles and Missions Review Report,* (Washington, DC: January 2009), 14 -15.

2. The following sources contributed to the scenario development: 624th Operation Center, Detachment 1, —Cyber Threat Bulletin: Phishing for Environmental Disaster in a Few Easy Steps;" Richard M. Crowell, —On War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare;" and William A. Owens, et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Full references provided below in bibliography.

3. 624th Operation Center, Detachment 1, —Cyber Threat Bulletin: Phishing for Environmental Disaster in a Few Easy Steps," *AF Portal*, 11 September 2009, https://www.my.af.mil/ (accessed 25 September 2009). –Supervisory Control and Data Acquisition, SCADA, is a computer system for gathering and analyzing real time data. These systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation."

4. Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-7 and 4-3. A Trojan horse is –a program that appears to be innocuous but in fact has a hostile function that is triggered immediately or when some condition is met."

5. Ibid., 2-13. –Onion routing works by establishing a path through a maze of multiple onion routers, each of which accepts a packet from a previous router and forwards it on to another onion router. The originating party—in this case, the attacker—encrypts the packet multiple times in such a way that each onion router can peel off a single layer of encryption; the final router peels off the last layer, is able to read the packet in the clear, and sends it to the appropriate destination."

6. Ibid., 2-25. –Although the direct effects of a cyberattack relate to computers, networks, or the information processed or transmitted therein, cyberattacks are often launched in order to obtain some other, indirect effect—and in no sense should this indirect effect be regarded as secondary or unimportant." Furthermore, the indirect or unanticipated effects may be far more important than the first-order effect against the computer.

7. Marie Brenner, –Preview of November 2009: Marie Brenner on the Taj Hotel Siege," *vanityfair.com*, http://www.vanityfair.com/politics/features/2009/11/taj-hotel-siege-2009, 3, (accessed 5 October 2009).

8. Jeremy Kahn, –Mumbai Terrorists Relied on New Technology for Attacks," *NYTimes.com*, 9 December 2008, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html (accessed 5 October 2009).

9. Marie Brenner, –Preview of November 2009: Marie Brenner on the Taj Hotel Siege," 6.

10. Jeremy Kahn, –Mumbai Terrorists Relied on New Technology for Attacks."

11. Marie Brenner, –Preview of November 2009: Marie Brenner on the Taj Hotel Siege," 12.

12. Ibid., 16.

13. Ibid., 1.

14. Ibid., 6. LeT goes by various names/spellings. Additional LeT information is found on the South Asia Terrorism Portal, —Lashkar-e-Toiba, Army of the Pure," (full reference in bibliography).

15. Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: CJCS, December 2006), 1. Document is now declassified.

16. Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: CJCS, 13 February 2006), II-4, 5. The Army, Navy, Air Force, Marines, and Defense Agencies all execute various elements of CNO to defend, exploit, attack, deceive, degrade, disrupt, and deny electronic information and infrastructure.

17. While the IO based doctrine provides a basic framework, it has not developed to capture the complex environment and expanding scope of cyberspace.

18. Every military Service and Agency relies on both internal and external networks for mission success. Essential computer systems span from relatively simple to very complex. Examples include internal aircraft, ship, spacecraft, and ground mobility operating systems, logistical systems, medical records, C2 of operational forces, intelligence collection and dissemination, and ubiquitous communications.

19. Joint Pub 3-13, *Information Operations*, II-5. Additionally, –This offers both opportunities to attack and exploit an adversary's computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation."

20. Gen James E. Cartwright, Acting Chairman of the Joint Chiefs of Staff, to Chiefs of the Military Services, memorandum, 18 August 2009.

21. DOD, *Quadrennial Roles and Missions Review Report*, 15.

22. Joint Pub 3-13, *Information Operations*, x.
23. Ibid., x.
24. Keith B. Alexander, ―Warfighting in Cyberspace," *Joint Forces Quarterly,* Issue 46, (3rd Quarter 2007): 60.
25. Joint Pub 3-13, *Information Operations*, II-5.
26. Ibid., GL-5.
27. Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, S-1. The document uses the one-word term ―cyberattack." From this point forward, this term is also used in the paper.
28. Ibid., 1-2. Furthermore, a cyberattack ―seeks to cause adversary computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary."
29. CJCS, *The National Military Strategy for Cyberspace Operations*, 2.
30. Joint Pub 3-13, *Information Operations*, GL-6.
31. Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, S-2. The document uses the one-word term ―cyberexploitation." From this point forward, this term is also used in the paper.
32. Ibid., 1-2.
33. CJCS, *The National Military Strategy for Cyberspace Operations*, 2.
34. Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-56.
35. Ibid., 2-54, 2-56, and 2-28. Additionally, a CNA ―may be designed to corrupt or degrade a system slowly—and exploitation is possible as long as the adversary does not notice the corruption." Furthermore, substantial amounts of intelligence about the targets (potentially gathered during CNE) are required if the attack is to be precisely directed against a specific system.
36. Rear Admiral William E. Leigher, (powerpoint presentation to the Information Operations Elective, Naval War College, Newport, RI, 16 October 2009). This figure is based upon an unclassified slide presented during the session. The author added the Operational Planning aspect.
37. Joint Pub 3-13, *Information Operations*, GL-5.
38. Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 3-9.
39. Charles W. Williamson III, ―Carpet bombing in cyberspace: Why America needs a military botnet," *Armed Forces Journal*, May 2008, http://www.armedforcesjournal.com/2008/05/3375884, (accessed on 10 October 2009). A botnet is ―a collection of widely distributed computers controlled from one or more points" that can be used to ―generate massive amounts of internet traffic and direct it against a small number of targets." The use of military botnets is theoretical only and there are several technological and legal issues, as described in the article.
40. After being added to the Axis of Evil list, a strategic objective of the NP attack was to terrorize, embarrass, and humiliate the United States in a highly visibility manner on the world stage (see page 2).
41. Joint Pub 3-13, *Information Operations*, I-1.
42. CJCS, *The National Military Strategy for Cyberspace Operations*, 5.
43. Ibid., 5.
44. Joint Pub 3-13, *Information Operations*, I-2.
45. For several years, senior DOD leaders have stated that cyberspace is a domain. In the 2006 *The National Military Strategy for Cyberspace Operations* (Secretary's Foreword), Secretary of Defense Donald Rumsfeld stated, ―the cyberspace domain is complex and evolves at astonishing rates, increasing the challenge of ensuring strategic advantage in this domain." (Full reference in bibliography)
46. Kevin P. Chilton, ―Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal*, Volume XXIII, Number 3, (Fall 2009): 5.
47. Alexander, ―Warfighting in Cyberspace," 60.
48. J. Kevin McLaughlin and Chris D. Crawford, ―Forward to the Future: A Roadmap for Air Force Space (Part II)," *High Frontier Journal*, Volume 4, Number 1, (November 2007): 29. Like cyberspace, space went through a similar domain debate. Space is now a recognized domain.
49. Michael W. Wynne, ―Flying and Fighting in Cyberspace," *Air and Space Power Journal*, (Spring 2007) http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/spr07/wynnespr07.html (accessed on 8 October 2009).

[50] Milan N. Vego, *Joint Operational Warfare: Theory and Practice*, (Newport, RI: Naval War College, Reprint 2009 (DVD), II-17.

[51] Ibid., II-19.

[52] Chilton, ―Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," 5. General Chilton observed that cyberspace is a crosscutting domain, global in nature and indifferent to any physical terrain or lines on a map.

[53] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 1-19.

[54] Ibid., 1-19.

[55] Ibid., C-1 to C-5. Appendix C provides examples of five cases ranging from a teenage hacker to sophisticated criminal groups. The cases discuss the extensive damage and costs caused by the hackers.

[56] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999, http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm (accessed on 14 October 2009).

[57] Vego, *Joint Operational Warfare: Theory and Practice*, II-19.

[58] CJCS, *The National Military Strategy for Cyberspace Operations*, 1. The NMS-CO states, ―the prosperity and security of our Nation rely on cyberspace to achieve strategic advantage and strengthen the instruments of national power. Cyberspace reaches across geopolitical boundaries and is tightly integrated into the operation of critical infrastructures and the conduct of commerce, governance, and national security."

[59] David T. Fahrenkrug, ―The Age of Cyber Warfare," *AF Portal*, 21 August 2008, https://www.my.af.mil/ (accessed 25 September 2009). ―From cell phones, to computers, to satellite television, society's very way of life has come to depend on the use of cyberspace." Moreover, the DOD relies on computer networks for almost all of its daily activities--from staff work to mission execution.

[60] Chilton, ―Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," 7. Additionally, many systems are linked using the Global Information Grid (GIG), giving soldiers, sailors, airmen, and marines the opportunity for information sharing and access to an infinite amount of data.

[61] CJCS, *The National Military Strategy for Cyberspace Operations*, 9. The NMS-CO states, ―DOD force transformation hinges largely on a move toward net-centric operations. Significant investments in force structure, infrastructure, and programs have oriented DOD components toward the use of cyberspace as an integral part of warfighting."

[62] Robert M. Gates, U.S. Secretary of Defense, to the Secretaries of the Military Departments, memorandum, 23 June 2009.

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] CJCS, *The National Military Strategy for Cyberspace Operations*, 10, 11. The NMS-CO summarizes required relationships and C2 by stating: ―The responsiveness, simplicity, agility, and flexibility of command relationships influence successful application of military power in cyberspace. Coordination of courses of action among combatant commanders is an on-going, collaborative process that begins with plan development and extends through operational execution...The United States can achieve superiority in cyberspace only if supported and supporting relationships are clearly defined and executed. These relationships must support unity of effort in achieving combatant commander missions as well as maintaining freedom of action in cyberspace. Senior leaders must establish a structure that integrates all mission areas and dismantles stove-piped organizations that hinder collaboration and lengthen decision-making cycles."

[67] Chairman, U.S. Joint Chiefs of Staff, *Command and Control for Joint Air Operations*, Joint Publication 3-30, (Washington, DC: CJCS, 5 June 2003), I-3. Joint Pub 3-30 summarizes this construct by stating, ―within one commander the responsibility and authority for planning, directing, and coordinating a military operation… the JFACC provides coherence, guidance, and organization to the air effort and maintains the ability to focus the tremendous impact of air capabilities/forces wherever needed across the theater of operations. Additionally, this assures the effective and efficient use of air capabilities/forces in achieving the JFC's objectives."

[68] U.S. Air Force, *Air Force Doctrine Document 1,* (Washington, DC: Department of the Air Force, 17 November 2003), 28.

[69] U.S. Strategic Command, ―Fact Sheet on Joint Functional Component Command for Space (JFCC-SPACE)," http://www.stratcom.mil/factsheets/space (accessed 16 October 2009).

[70] Ibid.

[71] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-2.

[72] Ibid., 2-35.

[73] Gates to the Secretaries of the Military Departments, memorandum. Additionally, Secretary Gates highlighted that USCYBERCOM —must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners."

[74] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-39.

[75] CJCS, *The National Military Strategy for Cyberspace Operations*, 11.

[76] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-2. Additionally, –the spatial scales may be anywhere from –concentrated in a facility next door" to globally dispersed."

[77] Ibid., 2-6.

[78] This is similar to execution of space mission requirements for a JFACC. The JFACC requests a capability and is normally provided Direct Liaison Authorized (DIRLAUTH) with the executing squadron. For example, a JFACC is not given Operational Control (OPCON) or Tactical Control (TACON) of the USAF Global Positioning System (GPS) squadron. The GPS mission, like cyberspace, has no boundaries and can simultaneously support multiple users. The author has over 14 years of USAF space experience.

[79] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-44.

[80] The NP cyber warriors used onion-routing and they also went through multiple countries to include the United States. Moreover, NP provided false tracks and hacked the AQ website to pass blame.

[81] Owens et al, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2-44.

[82] Ibid., 2-45. All-source attribution takes into account whatever information is available from efforts at technical attribution, but also uses information from other sources. Technical Attribution uses clues from the actual attack. Other all-source information may include intelligence, political sources, and other technical information (i.e., past attack tactics or signatures.)

[83] DOD, *Quadrennial Roles and Missions Review Report*, 15. Furthermore, it states, –The Department has made significant progress in operations in support of Combatant Commands and in working cyberspace issues collaboratively within the U.S. Government."

[84] Gates to the Secretaries of the Military Departments, memorandum.

[85] Over the last decade, JFCC-SPACE and the JSpOC have grown to better support GCC requirements. The Joint organization includes the Services, DOD agencies, and interagency and allied partners. The JSpOC has adapted and adjusted its C2 processes to meet the growing demand for space effects. The Space Tasking Order (STO) is an excellent C2 process example. The author has over 14 years of USAF space experience.

[86] Keith B. Alexander, –Warfighting in Cyberspace," 59.

[87] DOD, *Quadrennial Roles and Missions Review Report*, 14.

APPENDIX A

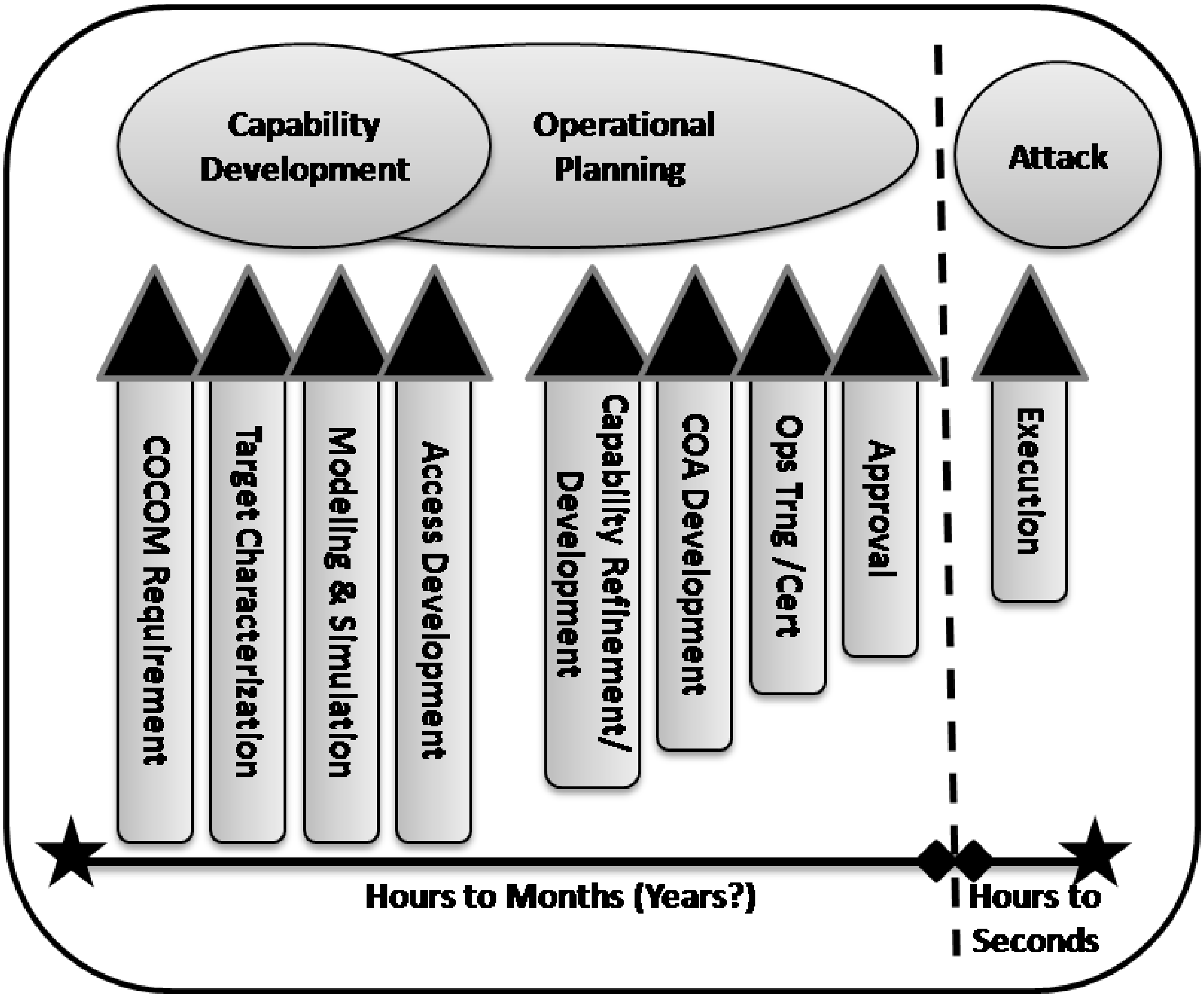

Figure 1 – CNE/CNA Process

APPENDIX A (continued)

Attribution Questions:
Was the cyberattack actually from AQ?
Do the tactics, techniques, and procedures (TTP) match past AQ attacks? Does it match AQ signature traits?
If not AQ, does the signature or TTPs match another known adversary?
Was the attack launched by agents of the NP government with the approval of the NP national command authorities?
Was the attack launched by low-level agents of the NP government without the approval or knowledge of the NP national command authorities?
Was the attack launched by NP citizens or ―patriotic hackers"? What action did the NP government take to stop them?
Were the NP computers controlled from an outside source (botnet)? Was the NP government framed?
Did the NP government ―contract" out the attack to a criminal organization to maintain deniability?
What response, if any, is appropriate against U.S. internet providers/servers (i.e., legal, denial of service, etc) during and/or after the cyberattack?

Table 1 – Cyberspace Attribution Questions

	JFCCC	**JFCC-Cyber**
Specialized Knowledge	***Low***	***High***
Coordination	***Medium***	***High***
Time	***Low***	***Medium***
Attribution Determination	***Low***	***Medium***
Contributes to Operational Vision	***Medium***	***High***

Table 2 – C2 Comparison Matrix

BIBLIOGRAPHY

624th Operation Center, Detachment 1. –Cyber Threat Bulletin: Phishing for Environmental Disaster in a Few Easy Steps.” *AF Portal*, 11 September 2009, https://www.my.af.mil/ (accessed 25 September 2009).

Alexander, Keith B. –Warfighting in Cyberspace.” *Joint Forces Quarterly,* Issue 46, (3rd Quarter 2007): 58-61.

Brenner, Marie. –Preview of November 2009: Marie Brenner on the Taj Hotel Siege.” *vanityfair.com*, http://www.vanityfair.com/politics/features/2009/11/taj-hotel-siege-2009 (accessed 5 October 2009).

Campen, Alan D. –Cyberwar Anyone?” *AF Portal*, 23 June 2008, https://www.my.af.mil/ (accessed 25 September 2009).

Cartwright, Gen James E. Acting Chairman of the Joint Chiefs of Staff. To Chiefs of the Military Services. Memorandum, 18 August 2009.

Chilton, Kevin P. –Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities.” *Air and Space Power Journal* XXIII, Number. 3, (Fall 2009): 5-10.

Crowell, Richard M. –On War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare.” Draft course material, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2009.

Fahrenkrug, David T. –The Age of Cyber Warfare.” *AF Portal*, 21 August 2008, https://www.my.af.mil/ (accessed 25 September 2009).

Gates, Robert M. U.S. Secretary of Defense. To the Secretaries of the Military Departments. Memorandum, 23 June 2009.

Kahn, Jeremy. –Mumbai Terrorists Relied on New Technology for Attacks.” *NYTimes.com*. 9 December 2008, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html (accessed 5 October 2009).

Krulak, Charles C. "The Strategic Corporal: Leadership in the Three Block War." *Marines Magazine*, January 1999, http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm (accessed on 14 October 2009).

Leigher, Rear Adm William E. Powerpoint presentation to the Information Operations Elective, Naval War College, Newport, RI, 16 October 2009.

McLaughlin, J. Kevin and Chris D. Crawford. –Forward to the Future: A Roadmap for Air Force Space (Part II).” *High Frontier Journal* 4, Number 1, (November 2007): 27-34.

Magnuson, Stew. ―Cyber-Attack.” *National Defense* XCIII, Number 668 (July 2009): 22-23.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, editors, Committee on Offensive Information Warfare, National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: The National Academies Press, 2009.

South Asia Terrorism Portal. ―Lashkar-e-Toiba, Army of the Pure.” http://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba.htm (accessed 19 October 2009).

U.S. Air Force. *Air Force Doctrine Document 1.* Washington, DC: Department of the Air Force, 17 November 2003.

U.S. Department of Defense. *Quadrennial Roles and Missions Review Report.* Washington, DC, January 2009.

U.S. Office of the Chairman Joint Chiefs of Staff. *Command and Control for Joint Air Operations*. Joint Publication 3-30. Washington, DC: CJCS, 5 June 2003.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, DC: CJCS, December 2006. Document is now declassified.

U.S. Strategic Command. ―Fact Sheet on Joint Functional Component Command for Space (JFCC-SPACE).” http://www.stratcom.mil/factsheets/space (accessed 16 October 2009).

Vego, Milan N., Dr. *Joint Operational Warfare: Theory and Practice*. U.S. Naval War College, Newport RI: Reprint 2009 (DVD).

Williamson, Charles W. III. ―Carpet bombing in cyberspace: Why America needs a military botnet.” *Armed Forces Journal*, May 2008, http://www.armedforcesjournal.com/2008/05/3375884 (accessed on 10 October 2009).

Wynne, Michael W. ―Flying and Fighting in Cyberspace.” *Air and Space Power Journal*. Spring 2007, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/spr07/wynnespr07.html (accessed on 8 October 2009).